

Amendments to the Drawings:

That attached sheets of drawings are believed to overcome the Draftperson's objections, and include the changes submitted with the Amendment filed April 25, 2004. These sheets, which include Figs. 1, 2, 3, 4, 5A, 5B, 6, 7A, and 7B, replace the original sheets included with the original application.

Attachment: Replacement Sheets

REMARKS

Claims 35-55 are all the claims pending in the application. The independent claims are 35, 42, and 49. No claims are amended, but new drawings are submitted to address the Draftperson's objection. This addresses each point of rejection raised by the Examiner. Favorable reconsideration is respectfully requested.

A. § 103(a) Rejection, Claims 35, 37-42, 44-49, and 51-55

Claims 35, 37-42, 44-49, and 51-55 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,205,437 to Gifford ("Gifford") in view of U.S. Publication No. 2004/0243520 to Bishop *et al.* ("Bishop") and U.S. Publication No. 2001/0044787 to Schwartz *et al.* ("Schwartz").

The Examiner acknowledges that Gifford does not disclose sending a challenge request to the buyer over the network, but asserts that in view of the disclosures of Bishop and Schwartz, one of ordinary skill in the art would have been motivated "to modify the method disclosed by Gifford to include the steps of sending a challenge request to the buyer over the network ... because it protects the network server from attacks and improve[s] the ease and safety of electronic commerce for consumers."

Applicants note that to the extent that the present claims are supported by Applicants' provisional application 60/198,110 filed April 17, 2000, both Bishop and Schwartz are prior art only to the extent that a complete embodiment of the subject matter cited by the Examiner can be found in one of the earlier provisional applications upon which Bishop and Schwartz are respectively based. Even so, Applicants have not undertaken a detailed analysis of the respective provisional applications at this time, as the present claims are believed to be patentable on the merits over the asserted combinations of references, for at least the following reasons:

1. There is no motivation to combine Gifford and Bishop, as the problem solved by Bishop was already solved in Gifford

In Gifford, a client computer requests a purchase by constructing "a payment order," adding an authenticator, and sending it for approval to a payment computer (*e.g.*, Gifford col. 8, lines 25-28). A payment order describes the identity of a sender, a payment amount, a beneficiary, and a sender unique nonce (Gifford col. 2, lines 59-61). A sender unique nonce is an identifier that is used only once by a given sender (Gifford col. 2, lines 63-64). An

example of sender unique nonces are unique timestamps (Gifford col. 2, lines 64-65). A public-key cryptographic signature is used as the authenticator (*see* Gifford col. 10, lines 30-42). The payment order is verified by using the public key known to the payment computer (*see* Gifford col. 8, lines 28-31; col. 10, lines 40-42). Replay attacks are prevented by checking to make sure the sender did not previously send a payment order with the same nonce. (Gifford, col. 8, lines 55-65).

In comparison, the purpose of cryptographic challenge in Bishop is to prevent replay attacks (Bishop, para. 0087: “Cryptographic challenge 1004 is any sort of challenge message that prevents replay attacks ... such as a challenge that is based upon random data and is designed to solicit a response from the X. 509 application stored on smartcard 202.”; *see also* Bishop, para. 0094: “Authentication server 306 ... then formats a challenge message 1106 (which may include random data)...”).

The express purpose of the challenge response in Bishop is to solve the problem of replay attacks, which was already solved by the invention of Gifford. There would have been no motivation to graft the challenge message feature of Bishop onto the invention of Gifford, as there is no problem to solve. Solving the same problem twice does not protect “the network server from attacks and improve the ease and safety of electronic commerce for consumers,” but rather, suggests that hindsight affected the selection of the art.

2. Contrary to the Examiner’s assertion, Bishop does not disclose displaying a challenge request to the buyer that is then digitally signed by the buyer

The Examiner states “Bishop et al. disclose sending a challenge request to the buyer over the network, the challenge request message to be displayed to the buyer then digitally signed by the buyer...” (para. 5 of Action). There is no suggestion that a component of the challenge message is to be displayed to the user and then digitally signed by the buyer. The cryptographic challenge in Bishop is “any sort of challenge message that prevents replay attacks (e.g., fraudulent messages created by re-sending previously sent authentication packets), such as a challenge that is based upon *random data* and is designed to solicit a response from the X.509 application stored on the smartcard 202.” (Bishop para. 0087; *see also* para. 0094 “...then formats a challenge message 1106 (which may include random data) ... The resultant signature request block is provided to smartcard 202 via reader 204. Smartcard 202 suitably signs the block and provides a copy of its X.509 certificate, as

appropriate.”). The only “display” to the user that Bishop discloses in relation to the challenge request is the option that the card reader 204 may interact with customer computer 110 “to prompt the user for a personal identifier, for example a personal identification number (PIN) or other unique identifier, to access the card.” (*See* Bishop para. 0089). This does not suggest the display and signing described in the claims.

3. Schwartz does not make up for the deficiencies of Gifford and Bishop

Shwartz discloses presentation of a window to the consumer “asking for approval of the transaction and presenting the challenge” (Shwartz para. 0182). The answer to the challenge is used to authenticate the consumer.

Applicants respectfully submit that the underlying teachings and problems addressed by Gifford are being ignored. The original payment order in Gifford includes an authenticator (nonce + encryption key), ensuring that the payment order was originated by the sender it describes. Bishop and Shwartz lack this initial verification, instead disclosing to rely upon a later challenge request to authenticate. Based on the disclosures of Bishop and Shwartz, there is no motivation whatsoever for one of ordinary skill to consider it desirable to re-authenticate an authenticated user.

Reconsideration and withdrawal of the § 103(a) rejection is requested.

B. § 103(a) Rejection, Claims 36, 43, and 50

Claims 36, 43, and 50 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Gifford, Bishop, and Shwartz, further in view of U.S. Publication No. 2001/0014158 to Baltzley (“Baltzley”).

Applicants submit that these claims are not obvious at least as further limitations on the independent claims. The combination of Gifford, Bishop, Shwartz, and Baltzley fails to overcome the deficiencies of Gifford, Bishop, and Shwartz.

C. Conclusion

Applicants authorize the Commissioner to charge any fees determined to be due with the exception of the issue fee and to credit any overpayment to Deposit Account No. 11-0600.

The Examiner is invited to contact the undersigned at (202) 220-4209 to discuss any matter concerning this application.

Respectfully submitted,
KENYON & KENYON

Dated: May 4, 2004



David A. Klein
Reg. No. 46,835

Kenyon & Kenyon
1500 K Street, N.W.
Suite 700
Washington, D.C. 20005
Tel: (202) 220-4200
Fax: (202) 220-4201

528595_1.DOC